UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/846,522	04/30/2001	Tomoyuki Nakano	112857-221	5535

29175 7590 03/07/2006

BELL, BOYD & LLOYD, LLC
P. O. BOX 1135
CHICAGO, IL 60690-1135

EXAMINER	
COLIN, CARL G	
ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 03/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/846,522	NAKANO ET AL.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 December 2005* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☒ The proposed drawing correction filed on *21 December 2004* is: a)☒ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 12/7/2005, applicant has amended claims 1, 5, 13, 14, 21, 22, and 23. The following claims 1-23 are presented for examination.

1.1 Applicant's arguments, pages 11-16, filed on 12/7/2005, with respect to the rejection of claims 1-23 have been fully considered, but they are not persuasive as amended. Applicant argues that the claimed invention as amended is patentable over the reference because Audebert discloses "a transaction signed by a terminal module using private key held by a card and because the terminal module decrypts the private key, signs transaction by means of the private key and sends the transaction to the PC". Examiner respectfully disagrees because that extract of information does not pertain to the scope of the invention disclosed by Audebert. Audebert discloses Applicant's scope of invention including mutual authentication between sender, (server), the authentication (terminal module), and the holding medium using public-key encryption method and common-key encryption method as explained in the rejection of the claims below. Therefore, Applicant has not overcome the rejection by amending the claims, and claims 1-23 remain rejected in view of Audebert.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

Claims 1, 13, 14, and 21-23 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

2.1 Claims 1, 13, 14, 21, and 23 recite the limitation "the authentication between the medium and a server". There is insufficient antecedent basis for this limitation in the claims.

Claims 1, 13, 14, 21, and 23 recite "the information processing apparatus or server authenticates the user using the private key corresponding to the user" and "...decrypted using the private key corresponding to the user ". It is not clear whether it is the same private key the information processing apparatus authenticates the user. In this case, there is a lack of consistency because according to the disclosure the information processing apparatus uses public key to authenticate the user and the authentication apparatus uses the private key (see page 11 of the specification).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to

which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3.1 **Claims 1-23** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,694,436 to **Audebert**.

3.2 **As per claims 1, 2, 4, 6-8, 10-18, and 20, Audebert** substantially discloses a user authentication system, comprising: an integrated circuit card that meets the recitation of a data holding medium for holding a common key unique to a user, used in a common-key encryption method, for example (see column 21, lines 17-21); for authentication between the data holding medium held by the user and a terminal module that meets the recitation of authentication apparatus (see column 26, lines 38-42) and a private key used in a public-key encryption method to the authentication between the data holding medium and a server or PC to perform a service to the user (see column 11, lines 10-29; column 12, lines 56-69 and column 24, lines 39-61); an authentication apparatus for holding the common key used in the common key encryption method and a private key used in a public-key encryption method, each unique to the user, for example (see column 21, line 45 through column 22, line 20); an information processing apparatus connected to the authentication apparatus in an always-communicable manner and provided with a function for performing authentication by the public-key encryption method, for example (see column 11, lines 10-29; column 12, lines 42-69 and column 24, lines 39-61); wherein the authentication apparatus performs authentication, authenticating the data holding medium by using the common key used in the common key encryption method for the user held

by the data holding medium, in response to an authentication request sent from the information processing apparatus, and, only when the user has been authenticated, performs processing for making the information processing apparatus authenticate the user by using the private key corresponding to the user, for example (see column 21, line 45 through column 22, line 20). **Audebert** discloses the authentication apparatus has means for authenticating the source and integrity of data received from the sender and further discloses using public-key encryption for secure communication (see column 23, lines 55 through column 24, line 22 and column 24, lines 23-64) that meets the recitation of wherein information encrypted by the public-key encryption method is sent from the information processing apparatus, forwarded to the authentication apparatus, decrypted using the private key corresponding to the user, so as to obtain decrypted information (see also column 21, lines 10-27 and lines 40-45 and column 25, lines 37-45); and discloses common key encryption method between the holding medium and the authentication apparatus that meets the recitation of wherein the decrypted information is encrypted means using the common key and wherein the obtained common key encrypted information is sent back to the data holding medium (see column 24, lines 40-45). **Audebert** clearly discloses the scope of the claimed invention as claimed and further suggests encrypting all data exchange between the modules (see column 24, lines 55-61) and further states encryption and signature mechanisms may be performed by any cryptographic techniques as known in the art (see column 12, lines 26-35). Although the steps are not explicitly disclosed with the exact orders as claimed, it would only require routine skill in the art to write the steps of the claimed invention using the encryption and authentication methods exchanged between the authentication apparatus, the holding medium, and information processing apparatus and the suggestions disclosed by

Audebert. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have information processing apparatus encrypting data and forwarding it for verification to the authentication apparatus since **Audebert** suggests that the holding medium does not have the cryptographic capabilities for signature, that the authentication apparatus contains (column 21, lines 10-26) and if data is verified sending it to the holding medium as suggested by **Audebert** (columns 23-24). One of ordinary skill in the art would have been motivated to do so as suggested by **Audebert** in order to perform a secure downloading of information into the medium that includes mutual authentication of all the modules involved (see column 23, lines 1-27).

As per claim 5, Audebert discloses a user authentication method for a user who carries an integrated circuit card that meets the recitation of a data holding medium for holding a common key unique to a user, used in a common-key encryption method, for example (see column 21, lines 17-21); for authentication between the data holding medium held by the user and a terminal module that meets the recitation of authentication apparatus (see column 26, lines 38-42) and a private key used in a public-key encryption method to the authentication between the data holding medium and a server or PC to perform a service to the user (see column 11, lines 10-29; column 12, lines 56-69 and column 24, lines 39-61); a method comprising discloses authenticating a data holding medium of a user by the common key encryption method using the common key held by the data holding apparatus in response to an authentication request from the server and performing only when the user has been authenticated processing for authenticating the user by a public-key encryption method (see column 21, line 45 through column 22, line 20;

see also another embodiment in columns 23-24). Therefore claim 5 is also rejected on the same rationale as the rejection of claim 1 above.

As per claims 3, 9, and 19, Audebert discloses the limitation of wherein the information processing apparatus is a mobile communication apparatus, for example (see column 27, lines 5-18).

Claims 21, 22 and 23 disclose similar limitations as the rejected claim 1 and are therefore rejected on the same rationale as the rejection of claim 1.

Conclusion

4. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

4.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cc

Carl Colin
Patent Examiner
March 6, 2006

CHRISTOPHER REVAK
PRIMARY EXAMINER

3/6/06